UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/560,641	12/13/2005	Johan Cornelis Talstra	NL 030753	6961

24737 7590 09/08/2008

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
ARCHER, CHRISTOPHER B	
ART UNIT	PAPER NUMBER
4148	
MAIL DATE	DELIVERY MODE
09/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/560,641	TALSTRA ET AL.	
	Examiner	Art Unit	
	CHRISTOPHER B. ARCHER	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/13/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 December 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/23/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 9 and 10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Regarding claim 9:

Claim 9 contains the term “bas key”, which is not described in the specification and is not well-known in the art.

Regarding claim 10:

Claim 10 contains the term “bas key”, which is not described in the specification and is not well-known in the art.

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 8:

Claim 8 recites the limitation "for every key-block" in paragraph 1, line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1 and 11-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Eskicioglu US (2002/0087865 A1), hereafter referred to as Eskicioglu.

Regarding claim 1:

Eskicioglu teaches "A method of establishing a secure authenticated channel between two devices device A and device B, where A authenticates to B using challenge/response public key cryptography, and device B authenticates to device A using zero-knowledge protocol" as **[(Eskicioglu paragraph [0010]) shows that challenge-response protocols based on symmetric or public key schemes, and zero-knowledge protocols are commonly used for mutual authentication]**.

Regarding claim 11:

Eskicioglu teaches "A system comprising a first device A and a second device B, where the device A is arranged to authenticate to the device B using

challenge/response public key cryptography, and the device B is arranged to authenticate to the device A using a zero-knowledge protocol" as **[(Eskicioglu paragraph [0010]) shows that two different parties can use challenge-response protocols based on symmetric or public key schemes, and zero-knowledge protocols are commonly used for mutual authentication]**.

Regarding claim 12:

Eskicioglu teaches "A first device A arranged to authenticate itself to a second device B using challenge/response public key cryptography, and arranged to authenticate the second device B using a zero-knowledge protocol" as **[(Eskicioglu paragraph [0010]) shows that two different parties can use challenge-response protocols based on symmetric or public key schemes, and zero-knowledge protocols are commonly used for mutual authentication]**.

Regarding claim 13:

Eskicioglu teaches "A second device B arranged to authenticate itself to a first device A using a zero-knowledge protocol, and arranged to authenticate the first device A using challenge/response public key cryptography" as **[(Eskicioglu paragraph [0010]) shows that two different parties can use challenge-response protocols based on symmetric or public key schemes, and zero-knowledge protocols are commonly used for mutual authentication]**.

Regarding claim 14:

"A computer program product comprising code enabling a programmable device to operate as the first device of claim 12" **[claim 14 is rejected under the same basis as claim 12, as claim 14 is merely a program designed to execute the process of claim 12]**.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eskicioglu in view of Menezes, van Oorschot and Vanstone, *Handbook of Applied Cryptography*, 1997 by CRC Press LLC, hereafter referred to as Menezes.

Regarding claim 2:

Eskicioglu teaches "The method of claim 1," but does not explicitly teach "in which the zero-knowledge protocol is a Guillou-Quisquater zero-knowledge protocol."

However, Menezes teaches "in which the zero-knowledge protocol is a Guillou-Quisquater zero-knowledge protocol" as **[(Menezes 412-414) shows**

that the Guillou-Quisquater zero-knowledge protocol is a common-zero knowledge protocol].

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Menezes into Eskicioglu as both deal with the common field of cryptography.

The ordinary skilled person would have been motivated to have applied the teaching of Menezes into Eskicioglu since Menezes describes different types of zero-knowledge authentication protocols.

Regarding claim 3:

Eskicioglu teaches “The method of claim 1," but does not explicitly teach “in which the zero-knowledge protocol is a Fiat-Shamir zero-knowledge protocol”.

However, Menezes further teaches “in which the zero-knowledge protocol is a Fiat-Shamir zero-knowledge protocol” as **[(Menezes 408-412) shows that the Fiat-Shamir zero-knowledge protocol is a common zero-knowledge protocol]**.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Menezes into Eskicioglu as both deal with the common field of cryptography.

The ordinary skilled person would have been motivated to have applied the teaching of Menezes into Eskicioglu since Menezes describes different types of zero-knowledge authentication protocols.

Regarding claim 4:

Eskicioglu teaches "The method of claim 1," but does not explicitly teach "in which the zero-knowledge protocol is a Schnorr zero-knowledge protocol".

However, Menezes further teaches "in which the zero-knowledge protocol is a Schnorr zero-knowledge protocol" as **[(Menezes 414-416) shows that the Schnorr zero-knowledge protocol is a common zero-knowledge protocol]**.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Menezes into Eskicioglu as both deal with the common field of cryptography.

The ordinary skilled person would have been motivated to have applied the teaching of Menezes into Eskicioglu since Menezes describes different types of zero-knowledge authentication protocols.

9. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Eskicioglu in view of Lotspiech et al. (US 6,118,873) hereafter referred to as Lotspiech.

Regarding claim 5:

Eskicioglu teaches "The method of claim 1," but it does not explicitly teach "in which device B authenticates to device A using a combination of the zero-knowledge protocol and a broadcast-encryption system, where a secret used in the zero-knowledge protocol is scrambled such that it can only be obtained by those that can process a broadcast encryption key-block successfully."

However, Lotspiech teaches "in which device B authenticates to device A using a combination of the zero-knowledge protocol and a broadcast-encryption system, where a secret used in the zero-knowledge protocol is scrambled such that it can only be obtained by those that can process a broadcast encryption key-block successfully" as **[(Lotspiech column 1 line 66 to column 2 line 17) shows a broadcast encryption scheme, in the form of a session key block, that only allows access to encrypted data to those who have the right to access said data)**.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Lotspiech into Eskicioglu as both deal with the common field of broadcast encryption.

The ordinary skilled person would have been motivated to have applied the teaching of Lotspiech into Eskicioglu since Lotspiech adds a method for formatting and transmitting the encryption keys to the authorized subscribers.

10. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eskicioglu in view of Lotspiech and further in view of Matyas, Jr. (US 6,102,287), hereafter referred to as Matyas Jr.

Regarding claim 6:

Lotspiech and Eskicioglu teach "the method of claim 5" but fail to explicitly teach "where the secret used in the zero-knowledge protocol is encrypted by the root-key K_{root} of a broadcast encryption system key-block."

However, Matyas Jr. teaches "where the secret used in the zero-knowledge protocol is encrypted by the root-key K_{root} of a broadcast encryption system key-block" as **[(Matyas Jr. column 15 line 56 to column 16 line 31) shows a key-block with a key for authentication]**.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Matyas Jr. into Eskicioglu as both deal with the common field of entity authentication.

The ordinary skilled person would have been motivated to have applied the teaching of Matyas Jr. into Eskicioglu since Matyas Jr. adds a method for formatting encryption keys and data.

Regarding claim 7:

Lotspiech and Eskicioglu teach "the method of claim 5" but fail to explicitly teach "where there is one key block with a root key, $K_{root,1}$ to allow for authentication, and another key block with root key $K_{root,2}$ for content encryption."

However, Matyas Jr. further teaches "where there is one key block with a root key, $K_{root,1}$ to allow for authentication, and another key block with root key $K_{root,2}$ for content encryption" as **[(Matyas Jr. column 15 line 56 to column 16 line 31) shows a key-block with two different encryption keys, one for authentication and one for content encryption]**.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have applied the teaching of Matyas Jr. into Eskicioglu as both deal with the common field of entity authentication.

The ordinary skilled person would have been motivated to have applied the teaching of Matyas Jr. into Eskicioglu since Matyas Jr. adds a method for formatting encryption keys and data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER B. ARCHER whose telephone number is (571)270-7308. The examiner can normally be reached on M-F 7:30-5 est..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THOMAS PHAM/
Supervisory Patent Examiner, Art Unit 4148

/CHRISTOPHER B ARCHER/
Examiner, Art Unit 4148